

**Amendment and Response**

Applicant: Norman C. Chou et al.

Serial No.: 10/057,159

Filed: January 24, 2002

Docket No.: 10011314-1/A310.258.101

Title: CONTROL OF AUTHENTICATION DATA RESIDING IN A NETWORK DEVICE

---

**| REMARKS**

The following remarks are made in response to the Office Action mailed August 30, 2005. Claims 1-34 were rejected. With this Response, claims 1, 2, 4, 6-8, 14, 19, 20 and 23-33 have been amended. Claims 1-34 remain pending in the application and are presented for reconsideration and allowance.

**Information Disclosure Statement**

Applicant notes that the Examiner has not considered the InfiniBand™ Architectures Specification Volume 1, Release 1.0, released October 24, 2000 by InfiniBand Trade Association cited in the specification of the Present Application, but did consider Infiniband Trade Association, Infiniband Architecture Specification Volume 1, Release 1.0.a, June 2001, chapters 1-3, 9, 11, 14-15 cited in the PTO-892 form.

**In the Drawings**

The Examiner has objected to the drawings for failing to comply with 37 C.F.R. 1.84(p)(5) because they include reference character(s) not mentioned in the description.

Applicants have amended the specification to now comply with the drawings. Applicants believe the drawings are now in condition for allowance.

In view of the above, Applicants respectfully request that the objections to the drawings be removed.

**In the Specification**

The Examiner has objected to the specification because of informalities. The Examiner has also objected to the specification because reference characters mentioned in the drawings are not mentioned in the specification.

Applicants have amended the specification identified by the Examiner. Applicants believe the specification is now in condition for allowance.

In view of the above, Applicants respectfully request that the objections to the Specification be removed.

**Amendment and Response**

Applicant: Norman C. Chou et al.

Serial No.: 10/057,159

Filed: January 24, 2002

Docket No.: 10011314-1/A310.258.101

Title: CONTROL OF AUTHENTICATION DATA RESIDING IN A NETWORK DEVICE**Claim Objections**

The Examiner objected to the claims 24-31, and 32 because of informalities.

Applicants have amended claims 24-31, and 32 to correct informalities. Applicants request reconsideration and withdrawal of the claim objections, and request allowance of these claims.

**Claim Rejections under 35 U.S.C. § 112**

The Examiner rejected claims 26 and 33 under 35 U.S.C. § 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Applicants have amended claims 26 and 33 to clarify these claims. Therefore, Applicants respectfully request that rejections to these claims under 35 U.S.C. § 112, second paragraph, be removed and that these claims be allowed.

**Claim Rejections under 35 U.S.C. § 101**

The Examiner rejected claims 22 and 24-31 under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter.

Applicant believes that claims 22 and 24-31 are directed to statutory subject matter. The specification describes, "method 600 is performed by processing logic, which may comprise hardware, software, or a combination of both." (see page 19, paragraph [43]). This implies that processing logic falls within statutory subject matter and therefore rejected claims 22 and 24-31 are allowable.

The Examiner rejected claims 33-34 under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter.

Applicants have amended the specification to conform the invention claimed in claims 33 and 34 to be within statutory subject matter.

In view of the above, claims 22, 24-31, and 33-34 are believed to be in form for allowance. Therefore, Applicants respectfully request that rejections to these claims under 35

**Amendment and Response**

Applicant: Norman C. Chou et al.

Serial No.: 10/057,159

Filed: January 24, 2002

Docket No.: 10011314-1/A310.258.101

Title: CONTROL OF AUTHENTICATION DATA RESIDING IN A NETWORK DEVICE

U.S.C. § 101, be reconsidered, and that the rejections be removed and that these claims be allowed.

**Claim Rejections under 35 U.S.C. § 103**

The Examiner rejected claims 1-32 under 35 U.S.C. § 103(a) as being unpatentable over the Infiniband Trade Association, (Infiniband Architecture Specification Volume 1, Release 1.0.a, June 19, 2001 (hereinafter "Infiniband" reference).

The Examiner rejected claims 33-34 under 35 U.S.C. § 103(a) as being unpatentable over the Infiniband Trade Association reference and further in view of the Susnow et al. U.S. Patent No. 2002/0159385.

The Examiner admits that the Infiniband Reference fails to teach the limitations of: amended independent claim 1 of a configuration switch; amended independent claim 8 of receiving a reset signal from a configuration switch at a decoder of a management port; independent claim 12 of refraining from sending subnet management packets (SMPs) to the management port upon detecting that the reset is required; receiving a message from the operator that indicates that the authentication data has been reset; independent claim 22 of means for refraining from sending subnet management packets (SMPs) to the management port upon detecting that the reset is required, means for receiving a message from the operator that indicates that the authentication data has been reset; amended independent claim 23 to receive a message from the operator that indicates that the authentication data has been reset; amended independent claim 33 of the machine-readable medium storing of description of a circuit and a plurality of units; and independent claim 34 of the computer readable medium comprising executable instructions, refraining from sending subnet management packets (SMPs) to the management port upon detecting that the reset is required, receiving a message from the operator that indicates that the authentication data has been reset.

Despite the lack of teaching of the above listed limitations of independent claims 1, 8, 12, 22, 23, 33, and 34 by the disclosure of Infiniband Reference cited by the Examiner, the Examiner nonetheless rejected claims 1, 8, 12, 22, 23, 33, and 34 under 35 U.S.C. § 103(a). Since the Examiner did not cite any other reference in rejecting these claims, the Examiner appears to be

**Amendment and Response**

Applicant: Norman C. Chou et al.

Serial No.: 10/057,159

Filed: January 24, 2002

Docket No.: 10011314-1/A310.258.101

Title: CONTROL OF AUTHENTICATION DATA RESIDING IN A NETWORK DEVICE

relying on official notice to teach the above listed limitations of these independent claims. Therefore, Applicants respectfully request allowance of these claims, or alternatively requests pursuant to MPEP § 2144.03 that the Examiner cite a reference to teach the above listed limitations of these independent claims.

In view of the above, Infiniband Reference does not teach or suggest each and every limitations of independent claims 1, 8, 12, 22, 23, 33, and 34.

Dependent claims 2-7 further define patentably distinct amended independent claim 1; dependent claims 9-11 further define patentably distinct amended independent claim 8; dependent claims 13-21 further define patentably distinct independent claim 12; dependent claims 24-26 further define patentably distinct independent claim 22; and dependent claims 27-32 further define patentably distinct amended independent claim 23. Therefore, these dependent claims are believed to be allowable.

Additionally, neither the Infiniband Reference nor the Susnow patent teach or suggest the limitations of amended independent claim 33 of a decoder configured to reset an authentication data stored in the decoder based on a reset signal received from a configuration switch, and to receive a management packet from a sub-network (subnet) manager with an update value for the authentication data residing in a plurality of units of an interconnect device. In addition, neither Infiniband Reference nor the Susnow patent teach or suggest the limitations of independent claim 34 of refraining from sending subnet management packets (SMPs) to the management port upon detecting that the reset is required; receiving a message from the operator that indicates that the authentication data has been reset.

By contrast, Infiniband Reference teaches a mechanism provided to authorize subnet management operations based on: a Key stored in the *MADHeader:M\_Key* of the LID routed and Directed route subnet management class datagram, a Key kept locally on each port in the *PortInfo:M\_Key* component of the *PortInfo* attribute. Authentication is performed by the management entity at the destination port and is achieved by comparing the key contained in the SMP with the key residing at the destination port. This key is known as the Management Key (M\_Key). A M\_Key contained in the *MADHeader:M\_Key* of the SMP shall not be checked at the receiving port if the *PortInfo:M\_Key* is set to zero, and as a result, no authentication is

**Amendment and Response**

Applicant: Norman C. Chou et al.

Serial No.: 10/057,159

Filed: January 24, 2002

Docket No.: 10011314-1/A310.258.101

Title: CONTROL OF AUTHENTICATION DATA RESIDING IN A NETWORK DEVICE

---

performed. If the *PortInfo:M\_Key* is nonzero, authentication at the receiving port and access to the port attributes is determined by the contents of the *PortInfo:M\_KeyProtectBits*. Finally, *M\_Keys* can be lost, so Key recovery is provided by the *PortInfo:M\_KeyLeasePeriod* components. (See Section 14.2.4 Management Key)

Infiniband Reference also teaches a Lease Period specified by setting the contents of the *Port-Info:M\_KeyLeasePeriod* component. It is intended to allow an *M\_Key* to 'expire' if the master SM inadvertently goes away without sharing the *M\_Key* backup SMs and there is no other out-of-band recovery mechanism available. The lease period timer shall start counting down toward zero on a port when a SMP is received for which the *M\_Key* check was performed according to Table 112 Protection Levels on page 655 and failed. If the lease timer countdown is already underway, it shall not be interrupted by the arrival of that SMP. The *PortInfo:M\_KeyViolations* component shall be incremented on a port when a SMP is received for which the *M\_Key* check was performed according to Table 112 and failed. The incrementing shall stop when the component reaches all 1s. Furthermore, if the port is capable of sending traps, a *M\_Key* violation trap described in Table 115 Traps on page 660 may be sent to the master SM indicating that the lease timer has started counting down. In response to that trap, the master SM may refresh the Lease Period. If the master SM that originally set the *M\_Key* has gone away, the Lease Period may expire. The lease period counter shall cease counting down and shall be reset to the value contained in *Portinfo:M\_KeyLeasePeriod* component on a port when any SMP is received with *MADHeader:M\_Key* that matches the *PortInfo:M-Key*. The *PortInfo:M\_KeyProtectBits* shall be set to zero when the lease period counter transitions from non-zero to zero. When the lease period expires, clearing the M-Key Protection bits will allow any SM to read (and then set) the M-Key. (See Section 14.2.4.2 Lease Period).

The Susnow patent teaches a software driver module that may be installed at the host-fabric adapter 120 to establish communication with a remote system (e.g., I/O controller), and perform functions such as host-fabric adapter initialization and configuration, channel configuration, channel abstraction, resource management, fabric management service and operations, send/receive IP transaction messages, remote direct memory access (RDMA) transactions (e.g., read and write operations), queue management, memory registration,

**Amendment and Response**

Applicant: Norman C. Chou et al.

Serial No.: 10/057,159

Filed: January 24, 2002

Docket No.: 10011314-1/A310.258.101

Title: CONTROL OF AUTHENTICATION DATA RESIDING IN A NETWORK DEVICE

descriptor management, message flow control, and transient error handling and recovery.  
(paragraph 41, lines 14-24)

With regard to independent claim 33, Infiniband Reference in no way teaches or suggests a decoder configured to reset an authentication data stored in the decoder based on a reset signal received from a configuration switch. Instead, Infiniband Reference teaches resetting of a lease period counter. Additionally, the Susnow patent does not teach or suggest a machine-readable medium storing a description of a circuit.

With regard to independent claim 34, Infiniband Reference in no way teaches or suggests detecting that a reset of authentication data residing in a management port of the interconnect device is required, and refraining from sending subnet management packets (SMPs) to the management port upon detecting that the reset is required. Additionally, the Susnow patent does not teach or suggest a computer readable medium comprising executable instructions; refraining from sending subnet management packets (SMPs) to the management port upon detecting that the reset is required; receiving a message from the operator that indicates that the authentication data has been reset.

In view of the above, the Infiniband Reference and the Susnow patent, do not teach or suggest alone or in combination all the limitations of independent claims 33 and 34.

Therefore, Applicants respectfully request reconsideration and withdrawal of the U.S.C. § 103(a) rejections to claims 1-34, and request allowance of claims 1-34.

**CONCLUSION**

In view of the above, Applicant respectfully submits that pending claims 1-34 are in form for allowance and are not taught or suggested by the cited references. Therefore, reconsideration and withdrawal of the rejections and allowance of claims 1-34 is respectfully requested.

No fees are required under 37 C.F.R. 1.16(b)(c). However, if such fees are required, the Patent Office is hereby authorized to charge Deposit Account No. 50-0471.

The Examiner is invited to contact the Applicant's representative at the below-listed telephone numbers to facilitate prosecution of this application.

**Amendment and Response**

Applicant: Norman C. Chou et al.

Serial No.: 10/057,159

Filed: January 24, 2002

Docket No.: 10011314-1/A310.258.101

Title: CONTROL OF AUTHENTICATION DATA RESIDING IN A NETWORK DEVICE

Any inquiry regarding this Amendment and Response should be directed to Patrick G. Billig at Telephone No. (612) 573-2003, Facsimile No. (612) 573-2005. In addition, all correspondence should continue to be directed to the following address:

**Agilent Technologies, Inc.**  
Intellectual Property Administration  
Legal Department, M/S DL429  
P.O. Box 7599  
Loveland, CO 80537-0599

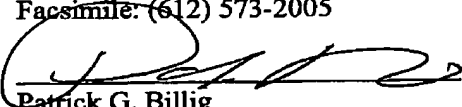
Respectfully submitted,

Norman Chou et al.,

By their attorneys,

**DICKE, BILLIG & CZAJA, PLLC**  
Fifth Street Towers, Suite 2250  
100 South Fifth Street  
Minneapolis, MN 55402  
Telephone: (612) 573-2003  
Facsimile: (612) 573-2005

Date: 11-30-05  
PGB:jan

  
Patrick G. Billig  
Reg. No. 38,080

**CERTIFICATE UNDER 37 C.F.R. 1.8:** The undersigned hereby certifies that this paper or papers, as described herein, are being facsimile transmitted to the United States Patent and Trademark Office, Fax No. (571) 273-8300 on this 30 day of November, 2005.

By   
Name: Patrick G. Billig